Leeor Neta, *admitted pro hac vice*
leeor@newmanlaw.com
Jake Bernstein, WSBA No. 39362
jake@newmanlaw.com
NEWMAN DU WORS LLP
2101 Fourth Avenue, Suite 1500
Seattle, WA 98121
Telephone: (206) 274-2800

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WASHINGTON

RIVER CITY MEDIA, LLC, a Wyoming limited liability company, MARK FERRIS, an individual, MATT FERRIS, an individual, and AMBER PAUL, an individual,

Plaintiffs,

v.

KROMTECH ALLIANCE CORPORATION, a German corporation, CHRIS VICKERY, an individual, CXO MEDIA, INC., a Massachusetts corporation, and STEVE RAGAN, an individual, and DOES 1-50

Defendants.

Case No. 2:17-cv-00105-SAB

FIRST AMENDED COMPLAINT

JURY TRIAL DEMANDED

RIVER CITY MEDIA, LLC ("River City"), MARK FERRIS ("Mark Ferris"), MATT FERRIS ("Matt Ferris"), and AMBER PAUL ("Paul") (collectively, "Plaintiffs") hereby allege for their complaint against CHRIS VICKERY ("Vickery"), KROMTECH ALLIANCE CORPORATION ("Kromtech"), CXO MEDIA, INC. ("CXO") (collectively, "Defendants") upon personal information as to Plaintiffs' own activities, and upon information and belief as to the activities of others, as follows:

I. PRELIMINARY STATEMENT

1. Since 2009, Matt Ferris, Mark Ferris, Amber Paul, and others have operated River City Media, LLC, a successful marketing company based in Eastern Washington. River City is used by some of the world's most recognizable brands, including MetLife, LifeLock, Liberty Mutual, Match.com, DirectTV, and Lyft.

2. River City consistently produces transparent, clean, and quality email marketing campaigns. River City has never been investigated—let alone sued—by anyone for violating regulations on email marketing. As such, River City has always had a sterling reputation in the industry.

3. But that reputation was destroyed after Defendants perpetrated a coordinated, months-long cyberattack against River City and its principals. The stated purpose was to destroy Plaintiffs' business and reputations.

4. One of the defendants, Chris Vickery, has a long history of using illegal methods to gain unlawful and unauthorized access to private databases and then publicizing his findings in order to make a name for himself as a security researcher.

5. Here, Vickery attacked River City's electronic infrastructure, spent months worming his way through River City's networks, collected confidential, proprietary, and sensitive data, and used it to intentionally harm River City's information technology systems.

6. Vickery then convinced the remaining Defendants to assist him in

publicizing and "exposing" Plaintiffs by publishing multiple false and defamatory articles on their blogs and news websites. This served only to compound and magnify the harm caused by the cyberattack on River City's digital infrastructure.

7. Defendants' illegal actions caused immense damage to Plaintiffs' businesses, reputations, livelihoods, and physical and mental health. River City is now on the verge of collapse. And anyone on the internet can access the personal and private information of River City's principals.

8. Plaintiffs bring this action to salvage their reputation, recover their damages, and prevent Defendants from victimizing them—or anyone else—in the future.

II. JURISDICTION AND VENUE

9. This Court has jurisdiction over this action under 28 U.S.C. § 1332(a) because the matter in controversy exceeds the sum or value of $75,000 and is between citizens of different States.

10. This Court also has jurisdiction over this action under 28 U.S.C. § 1331 because this matter arises under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

11. This Court also has jurisdiction over this action under 28 U.S.C. § 1331 because this matter arises under the Stored Communications Act, 18 U.S.C. § 2701 et seq.

12. This Court also has jurisdiction over this action under 28 U.S.C. § 1331 because this matter arises under the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq.

13. This Court also has jurisdiction over this action under 28 U.S.C. § 1331 because this matter arises under the Defend Trade Secrets Act, 18 U.S.C. § 1832 et seq.

14. This Court may exercise supplemental jurisdiction over the state law claims made herein under 28 U.S.C. § 1367 because they are so related to claims in

NEWMAN DU WORS LLP
2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

the action within this Court's original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

15. This Court has personal jurisdiction over Defendants Vickery and Ragan because they purposefully directed their activities in Washington, and because Plaintiffs' claims arise and relate to Vickery and Ragan's activities directed at Washington.

16. This Court has personal jurisdiction over Defendant CXO because CXO has or had the right to substantially control Vickery and Ragan's activities. Vickery himself admits that he, Ragan and CXO worked as a "team" to access Plaintiffs' servers and cause Plaintiffs' damage. This "team" shared Plaintiffs' data with each other leading to the publication of articles that damaged Plaintiffs. There is no question that Ragan is an employee of CXO Media, Inc. Nor is there any question that CXO Media, Inc. had the right to control Ragan's activities. CXO has also submitted to this Court's jurisdiction. (*See* ECF No. 107.)

17. This Court has personal jurisdiction over Defendant Kromtech because Kromtech has or had the right to substantially control Vickery's activities. Kromtech owns, operates and sponsors the website MacKeeper.com, home to the MacKeeper.com Security Research Center and blog. At all times relevant to this lawsuit, Vickery was a "MacKeeper Security Researcher." He wrote articles for MacKeeper.com, which Kromtech posted publicly. Kromtech admits that it hired Vickery to "provide two articles each month; one article on a data breach, the other on a general security topic." At least one of those articles was based on data that Vickery—as an agent of Kromtech—unlawfully obtained from River City's servers and networks during a months-long hacking campaign. Acting on behalf of Kromtech, Vickery stole, analyzed, and published nearly all of River City's sensitive and proprietary data. Based on that data, Vickery then spread false, defamatory, and reputation-ruining information about River City on the website, MacKeeper.com, which is owned, operated, and sponsored by Kromtech. By

NEWMAN DU WORS LLP
2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

employing Vickery and providing him with a mandate and platform on which to publicize his illegal hacking, Kromtech is directly responsible for Plaintiffs' damages. Kromtech is also subject to this Court's jurisdiction because it circulated Vickery's and other articles within the state of Washington, where Kromtech marketed and sold a significant number of units of products and services.

18. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events giving rise to the claims occurred within this judicial district and because Defendants directed their illegal computer access activity to protected computers within this judicial district.

III. PARTIES

19. Plaintiff River City Media, LLC is a Wyoming limited liability company with its principal place of business in Liberty Lake, Washington.

20. Plaintiff Matt Ferris is an Idaho resident and a member of and Chief Executive Officer for River City Media, LLC.

21. Plaintiff Mark Ferris is an Idaho resident and a member of and Chief Technology Officer for River City Media, LLC.

22. Plaintiff Amber Paul is an Idaho resident and Chief Marketing Officer for River City Media, LLC.

23. Defendant Chris Vickery is a California resident and works as a "security researcher" for MacKeeper.com, which is owned and operated by Defendant Kromtech.

24. Defendant Kromtech is a German company headquartered in Dubai. Kromtech owns and operates the website MacKeeper.com and the apps and services of the same name. Kromtech maintains offices in New Orleans, Louisiana and avails itself of the privileges of conducting activities within the United States.

25. Defendant CXO is a Massachusetts corporation and the owner and operator of the website www.csoonline.com, a security and technology news blog.

26. Plaintiffs are unaware of the true names and capacities of the

defendants identified as Does 1–50 and therefore sues those defendants under fictitious names. Plaintiffs will amend this complaint to allege their true names and capacities when ascertained. Each of the fictitiously-named defendants is responsible for the conduct alleged herein. These fictitiously-named defendants, along with the other named defendants, are referred to collectively as "Defendants."

27. Each defendant aided and abetted the actions of the other defendants set forth above, in that each defendant had knowledge of those actions, and provided assistance and benefitted from those actions. Each of the defendants was the agent of each of the other defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of the other defendants.

IV. STATEMENT OF FACTS

A. Introduction

28. River City is an internet-based marketing company located in Eastern Washington. It is operated by Matt Ferris, Mark Ferris, Amber Paul, and others.

29. Since 2009, the Ferrises, Paul, and others have built River City into a successful and well-reputed company, working on behalf of numerous, globally recognized brands.

30. Defendant Chris Vickery is a self-styled "security researcher" who worked as an IT help desk technician until he claimed to have "stumbled upon" allegedly publicly exposed databases used by MacKeeper.com (owned by Defendant Kromtech).

31. Defendant Kromtech operates MacKeeper.com and owns the product known as MacKeeper, an app for cleaning, optimizing, and securing Mac

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

computers. MacKeeper is known to have a dubious reputation.[1]

32. After Vickery illegally accessed Kromtech's data systems, Kromtech chose to hire Vickery as a "security researcher" because it believed he was uniquely situated to help them secure their proprietary information.

33. At all times relevant hereto, Vickery worked for Kromtech and maintained a MacKeeper.com Security Research Center and blog.

34. As more fully explained below, Vickery has a history of improperly accessing private databases without authorization and publicizing his findings in order to promote himself as a "successful" security researcher.

35. At base, Vickery is a vigilante black-hat hacker who breaks into data systems without authorization or consent and exposes confidential, sensitive, and proprietary information, both intentionally and recklessly.

B. Chris Vickery's Hacking History

36. Vickery is not and never has been a certified security professional. He spends his time scouring the web for private databases to which he can gain access. If he finds something interesting, he downloads and publishes it. Vickery employs specialized software to find and access private databases without permission.

37. Vickery's activities are no secret. He has even gone on record regarding his illegal tactics. For example, he admitted to the BBC that he initiated an unlawful attack on uKnowKids.com in February 2016.[2]

38. Regardless of his motives and the difficulty involved, Vickery has repeatedly violated state and federal law by gaining access to computer systems without authorization and using that access to damage companies and destroy

---

1 See, e.g., "Q: Is Mackeeper a legitimate program?", Official Apple Discussion Forums, available at https://discussions.apple.com/thread/4276731?tstart=0, last visited March 17, 2017.

2 *See* Zoe Kleinman, "Child tracker firm in 'hack' row", BBC News, available at http://www.bbc.com/news/technology-35639545, last visited March 21, 2017.

reputations.

39. As described below, Vickery's recent cyberattack on River City is just another example of his unlawful activities, recognized as unjustified by the very security profession he claims to represent.

C. Defendants' Computer Hacking Campaign

40. Defendant CXO is a media company that runs http://www.csoonline.com/, a security-focused news blog. Defendant Ragan is a "Senior Staff Writer" at CSO and writes for the "Salted Hash" security blog.

41. On March 6, 2017, Defendants CXO and Ragan posted the following statement to CXO's "Salted Hash" security blog: "This is the story of how River City Media… accidentally exposed their entire operation to the public after failing to properly configure their rsync backups."

42. In this (and other) articles more fully described below, Defendants claim that River City misconfigured a type of computer backup system and accidentally exposed its entire system to the public.

43. In fact, River City's records show that Defendants systematically infiltrated River City's data network, illegally gained access to River City's databases without authorization, and then copied, modified, and damaged River City's confidential, sensitive, and proprietary information.

44. River City determined that it first became the victim of an illegal hacking campaign on or about January 16, 2017, when its Google Scripts account was presented with a login challenge from an IP address belonging to a provider of "Private Internet Access." This is a type of anonymous internet connection often used by hackers.

45. An "IP address"—or internet protocol address—is a numerical identifier that acts as the "mailing address" for computers on the internet. Any computer that connects to the internet needs a unique IP address in order to receive the "packets" addressed to it. The internet uses two versions of the IP

address system: v4 and v6. In most cases, IPv4 is still the most relevant type and appears as four numbers separated by a period, with each number ranging from 0 to 255. For example, a common IP address used within local networks is 192.168.0.1.

46. IP addresses change depending on the network a person uses to connect to the internet. For example, the IP address for a computer connecting to the internet via public wifi at a library will be different than that same computer's IP address when it connects to the internet from home.

47. By examining the IP addresses of computers connecting to its network, River City (or any other victim of a cyberattack) can identify which connections are valid and which connections are not.

48. In fact, IP address restrictions are often used to create "Access Control Lists" (ACL), which are simply lists of IP addresses that are expressly authorized to log into and access certain systems. If a person uses an IP address not listed on the ACL, that person is denied access. If that person nonetheless gains access, his access is, by definition, without authorization. River City secured some of its network assets with ACLs, which Defendants intentionally bypassed.

49. River City detected the first successful login to its systems from a suspicious IP address on or about January 27, 2017.

50. This threat agent[3] often connected to River City's network using "private internet access" (PIA), which is an intentionally untraceable IP address used by hackers to hide their identities. Other times, such as on January 24, 2017, the threat agent logged in via an IP address (172.81.159.131) traced to the Axiom Hotel in San Francisco, California.

51. Until Defendants publicly announced their unlawful computer hacking, River City did not know the identities of these threat agents. Plaintiffs now

[3] In computer security, a threat agent is the generic term for an entity that can exploit a vulnerability.

believe that all threat agents were, in fact, Vickery or those working with or for Vickery.

52. Although it could not initially determine the hackers' identities, River City could still log their activities. On January 28, 2017, a then-unknown threat agent connected to River City's "Zabbix" server[4] via an IP address from the 104.200.154.x block,[5] which belongs to Total Server Solutions, LLC, a managed server and cloud company that provides private internet access. This threat agent spent several days inside River City's Zabbix server, learning as much as it could about River City's network before ultimately using that information to compromise additional River City computer systems.

53. River City's Zabbix server is used to monitor River City's network for possible irregularities and intruders. By purposefully attacking and compromising River City's Zabbix server, Defendants effectively hamstrung River City's ability to detect and stop their cyberattack.

54. Defendants also accessed and destroyed data on River City's "netbox," a specific server that kept records of River City's network topology. Without this "map" of its network, River City lost the ability to manage its own systems, causing severe service disruptions and making recovery of River City's network much more difficult.

55. If Defendants had simply "stumbled upon" River City's backup

---

[4] Zabbix is an open-source networking and application monitoring application used to track the status of various network services, servers, and other network hardware. *See* http://www.zabbix.com/product, last visited March 13, 2017.

[5] IP (Internet Protocol) addresses are assigned by "block" and this information is maintained by the American Registry for Internet Numbers (ARIN) located at http://www.arin.net/. The ARIN database is publicly accessible and indicates which organization is responsible for which blocks during a given time period. For example, as of March 21, 2017, the block 50.181.0.0 ¬– 50.181.127.256 was assigned to Comcast Cable Communications Holdings, Inc. *See* https://whois.arin.net/rest/net/NET-50-181-0-0-1, last visited March 21, 2017.

NEWMAN DU WORS LLP
2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

database (as Vickery claims), there would have been no need to attack and compromise one of River City's primary intrusion detection systems nor to purposefully destroy the "netbox," deleting files critical to River City's operations.

56. On or about February 5, 2017, the same threat agent—Vickery—accessed the "rcm dev" system using cryptographically-secured credentials that Vickery could only have obtained from his prior illegal access.

57. River City exported a history of all commands entered into its Linux-based servers and systems as part of its investigation into the hacking campaign (the "Bash History").

58. The Bash History is a text log of all command line inputs entered by the threat agent on various Linux computers and it shows the systematic exploration of River City's Linux-based computers. This type of systematic exploration would only be performed by an unauthorized intruder.[6]

59. Defendants did much more than simply copy and publish Plaintiffs' private data. Once they gained access to River City's systems, they located and used River City's credentials for its: (1) company email accounts; (2) its Dropbox.com account; (3) its accounts for affiliate networks; (4) its PayPal accounts; (5) its Hipchat accounts; (6) its email service provider accounts; and (7) its Github accounts. None of these accounts were exposed to the public but all were accessed without authorization by the same threat agent.

60. Defendants also used River City's PayPal account to make unauthorized purchases at http://www.alpnames.com/, a domain registrar. With

[6] For example, the Bash History is replete with "cd" and "ls" commands. These commands are used to change the working directory and list all files within the working directory respectively. An intruder uses these commands to navigate a system and "look around." An authorized user would already know how to get around and generally would not need to use such commands.

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

ALPNames.com's assistance, River City traced the unauthorized activity to mailto:blueshield@protonmail.com. Vickery is known to use a "protonmail.com" email address.[7]

61. Defendants had no authority to misappropriate and convert the funds that River City had stored in its PayPal account.

62. Ultimately, Defendants used the data that they obtained to attack and damage River City's reputation via media and blog postings.

63. Defendants also used the data that they obtained to log in to River City's email service provider accounts and then draft and send illegal emails. For example, Defendants sent offensive emails that appeared to come from one of River City's principals, Alvin Slocombe. These emails had the false and misleading subject line of "Donald Trump's Transvestite Surprise" and an offensive email body that stated "Try and Stop Me Bitch."

64. Vickery admits to looking for "suspicious data," which he claimed to have found "publicly exposed" on an "rsync server" via Port 873.

65. But Defendants could not have "stumbled upon" River City's data as they contend. In fact, Defendants illegally accessed River City's IT infrastructure via the lengthy and highly coordinated cyberattack described above.

D. Defendants' Media Campaign

66. After its coordinated black-hat cyberattack, Defendants launched a media campaign intended to destroy River City's reputation and to eliminate it as a viable business.

67. On March 6, 2017, Defendants published the following news articles, both of which contain multiple libelous and false statements about Plaintiffs (collectively the "Defamatory Stories"):

[7] When River City sent cease and desist letters to Defendants, Vickery responded to River City with his *cvickery@protonmail.com* account.

a. "Spammergate: The Fall of an Empire" by Chris Vickery posted at https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire (the "Vickery Article");

b. "Spammers expose their entire operation through bad backups" by Steve Ragan posted at http://www.csoonline.com/article/3176433/security/spammers-expose-their-entire-operation-through-bad-backups.html (the "Ragan Article");

68. The Vickery and Ragan Articles paint River City as an illegal—even *criminal*—spam operation that allegedly uses "illegal hacking" techniques to send "up to a billion daily emails."

69. This negative publicity has caused and continues to cause River City to lose contracts, suffer canceled leases, and lay off employees. River City's business partnerships have been destroyed. In short, Defendants have caused and continue to cause irreparable harm to River City.

70. If that were not enough, River City's principals and employees have suffered significant personal injury. Until recently, Plaintiff Amber Paul also served as the CEO of Persistent Media, a subsidiary of Tax Law Solutions. Because of Defendants' defamatory statements, the majority shareholders asked Paul to resign and told her that they needed her as "far away as possible" from their company. The additional stress caused by the loss of her position resulted in further emotional stress and financial damage to Paul.

71. Because of information exposed by Defendants to the public, outside forces also attacked the security cameras at Matt Ferris's private residence.

E. The Vickery and Ragan Articles

72. As indicated Defendants published the Vickery and Ragan Articles, both of which contained numerous false statements about River City.

73. The Vickery Article makes the following false and defamatory

statements about River City's marketing practices:

a. "River City masquerades as a legitimate marketing firm while, per their own documentation, being responsible for up to a billion daily email sends."

b. "How can a group of about a dozen people be responsible for one billion emails sent in one day? The answer is a lot of automation, years of research, and a fair bit of illegal hacking."

74. The Vickery Article also falsely accuses River City of engaging in "a type of Slowloris attack"—a type of black-hat maneuver.

75. For its part, the Ragan Article makes the following false and defamatory statements about River City's marketing practices:

a. Quoting Vickery, "Once we concluded that this was indeed related to a criminal operation…"

b. River City "exploit[ed] a number of providers in order to inbox offers."

c. Quoting Spamhaus's Mike Anderson: "Nobody would knowingly give their email address to spammers, so they have to be tricked into it…the original contract for handing over the address is never fulfilled, since it turns out to be impossible to redeem the 'free gift' or only with extreme difficulty."

76. In addition, the Ragan Article links to the Vickery Article on MacKeeper.com, thereby incorporating and/or adopting the statements contained the Vickery Article.

77. The statements described above are false. River City is not an illegal spam operation. River City does not engage in criminal computer hacking. River City sends nothing close to a billion emails each day. River City does not use scripts to abuse email services. River City does not and has never engaged in "Slowloris" attacks.

78. Instead, River City is the victim of an illegal hacking campaign that Defendants used to expose River City's proprietary and private data to the public for no other reason it seems than to "make news."

F. River City's Cease and Desist Letters

79. On March 12, 2017, River City directed its legal counsel to issue cease and desist letters to the parties named in this lawsuit, as well as AOL, Inc., because of an article posted on its tech blog, www.techcrunch.com.

80. The cease and desist letters requested that Defendants and non-party AOL, Inc. remove the Defamatory Articles, publicly retract the accusations made against River City and apologize to River City.

81. Defendant Vickery responded, stating that he had committed no criminal act nor stated anything "without good reason to state it." He also refused to retract the Vickery Article.

82. Shortly after sending this response, Vickery boldly threatened to expose more of River City's proprietary and private files on his Twitter account: "For every legal threat, more will be shared from [River City]'s own exposed files…" This post included a link to a Dropbox.com folder containing confidential information, including private banking information.

83. In addition to this threat to release more data in the future, Vickery has *already* distributed a substantial amount of River City's data on several hacker-friendly websites called "leak forums."

V. FIRST CAUSE OF ACTION

(Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

84. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

85. Defendant Vickery is not an employee or authorized user of River City's computer networks.

86. Vickery intentionally and without authorization gained access to

confidential and sensitive information stored on River City's private computer network, which at all relevant times operated in and affected interstate and foreign commerce and accordingly are considered protected computers.

87. Without authorization or permission, Vickery obtained tens of thousands of confidential, proprietary, and sensitive business records, including account credentials, client records, email lists, and other records containing sensitive business and personal information.

88. Without authorization or permission, Vickery used confidential account credentials to unlawfully access River City's payment accounts and used River City's funds to make purchases without River City's knowledge, consent, or authorization.

89. Without authorization or permission, Vickery intentionally accessed River City's protected computers and intentionally or recklessly caused damage to River City's protected computers, which resulted in loss and damages to River City.

90. Vickery took all such actions knowingly and intentionally and without regard for the rights of others.

91. Vickery undertook these actions personally, and with the knowledge, approval and/or ratification of Kromtech, CXO, Ragan, and the remaining defendants.

92. As a direct and proximate result of Defendants' unlawful and improper conduct, River City has suffered losses exceeding $5,000 during the period between January 15, 2017 and the present, and continuing thereafter.

VI. SECOND CAUSE OF ACTION

(Violations of the Stored Communications Act, 18 U.S.C. § 2701 et seq.)

93. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

94. Defendant Vickery is not an employee or authorized user of River

City's computer networks.

95. Vickery intentionally and without authorization gained access to confidential and sensitive information stored on River City's private computer network, which at all relevant times operated in and affected interstate and foreign commerce and is accordingly considered a protected computer.

96. Without authorization or permission, Vickery obtained tens of thousands of confidential, proprietary, and sensitive business records, including account credentials, client records, email lists, and other records containing sensitive business and personal information.

97. Without authorization or permission, Vickery used confidential account credentials to unlawfully access River City's payment accounts and used River City's funds to make purchases without River City's knowledge, consent, or authorization.

98. Vickery took all such actions knowingly and intentionally and without regard for the rights of others.

99. Vickery undertook these actions personally, and with the knowledge, approval and/or ratification of Kromtech, CXO, Ragan, and the remaining defendants.

100. As a direct and proximate result of Defendants' unlawful and improper conduct, River City has suffered losses exceeding $5,000 during the period between January 15, 2017 and the present, and continuing thereafter.

101. River City alleges that punitive and exemplary damages are appropriate because Defendants' actions were willful, malicious, oppressive, and fraudulent, in willful and conscious disregard of River City's rights and have subjected River City to cruel and unjust hardship.

102. Under 18 U.S.C. § 2707(c), River City also seeks its attorney's fees associated with the investigation and prosecution of this action.

VII. THIRD CAUSE OF ACTION

(Violations of the Defend Trade Secrets Act, 18 U.S.C. § 1832 et seq.)

103. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

104. Defendant Vickery is not an employee or authorized user of River City's computer networks.

105. Vickery intentionally and without authorization gained access to confidential and sensitive information stored on River City's private computer network, which at all relevant times operated in and affected interstate and foreign commerce and is accordingly considered a protected computer.

106. Without authorization or permission, Vickery obtained tens of thousands of confidential, proprietary, and sensitive business records, including account credentials, client records, email lists, and other records containing sensitive business and personal information, all of which constitute trade secrets used in interstate or foreign commerce under 18 U.S.C. § 1839(3).

107. Vickery took all such actions knowingly and intentionally and without regard for the rights of others.

108. Vickery undertook these actions personally, and with the knowledge, approval and/or ratification of Kromtech, CXO, Ragan, and the remaining defendants.

109. Defendants' therefore knowingly acquired Plaintiffs' trade secrets by improper means and knowingly disclosed Plaintiffs' trade secrets obtained by improper means.

110. Defendants' conduct constitutes misappropriation of Plaintiffs' trade secrets under 18 U.S.C. § 1836(b)(1).

111. Plaintiffs have been damaged, and continue to be damaged, by Defendants' unlawful conduct.

VIII. FOURTH CAUSE OF ACTION

(Violations of the Electronic Comm'ns. Privacy Act, 18 U.S.C. § 2510 *et seq.*)

112. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

113. Defendant Vickery is not an employee or authorized user of River City's computer networks.

114. Vickery intentionally and without authorization gained access to confidential and sensitive information stored on River City's private computer network, which at all relevant times operated in and affected interstate and foreign commerce and is accordingly considered a protected computer.

115. Without authorization or permission, Vickery obtained tens of thousands of confidential, proprietary, and sensitive business records, including account credentials, client records, email lists, and other records containing sensitive business and personal information.

116. Vickery took all such actions knowingly and intentionally and without regard for the rights of others.

117. Vickery undertook these actions personally, and with the knowledge, approval and/or ratification of Kromtech, CXO, Ragan, and the remaining defendants.

118. As a direct and proximate result of Defendants' unlawful and improper conduct, River City has suffered losses exceeding $5,000 during the period between January 15, 2017 and the present, and continuing thereafter.

119. River City alleges that punitive and exemplary damages are appropriate because Defendants' actions were willful, malicious, oppressive, and fraudulent, in willful and conscious disregard of River City's rights and have subjected River City to cruel and unjust hardship.

IX. FIFTH CAUSE OF ACTION

(Invasion of Privacy)

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

120. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

121. Vickery intentionally and without authorization gained access to confidential and sensitive information stored on River City's private computer network, which at all relevant times operated in and affected interstate and foreign commerce and is accordingly considered a protected computer.

122. Without authorization or permission, Vickery obtained tens of thousands of confidential, proprietary, and sensitive business records, including account credentials, client records, email lists, and other records containing sensitive business and personal information.

123. Vickery undertook these actions personally, and with the knowledge, approval and/or ratification of Kromtech, CXO, Ragan, and the remaining defendants.

124. All Defendants then used the information illegally obtained by Vickery to give publicity to matters concerning the private lives of each Plaintiff.

125. The matters publicized by Defendants are highly offensive to a reasonable person and are not of legitimate concern to the public.

126. As a result of Defendants' unlawful invasion of their privacy, Plaintiffs have suffered, and continue to suffer, damages in an amount to be determined at trial.

X. SIXTH CAUSE OF ACTION

(Intentional Interference with Contractual Relationships)

127. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

128. Plaintiffs maintained numerous contractual relationships with multiple business partners, service providers, and customers.

129. To obtain and maintain these relationships, Plaintiffs endured lengthy vetting processes and have adhered to strict compliance guidelines. Plaintiffs'

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

business partners considered River City a "top tier" partner.

130. Defendants knew about these contractual relationships.

131. Defendants intentionally interfered with Plaintiffs' contractual relationships by improper means, namely unlawful computer access in violation of multiple state and federal statutes.

132. Defendants' intentional interference caused and continues to cause damage to Plaintiffs.

XI. SEVENTH CAUSE OF ACTION

(Intentional Interference with Business Expectancy)

133. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

134. Plaintiffs continuously signed new clients and obtained new contracts, all of which constitute valid business expectancies.

135. Defendants knew about these business expectancies.

136. Defendants intentionally interfered with Plaintiffs' business expectancies by improper means, namely unlawful computer access in violation of multiple state and federal statutes.

137. Defendants' intentional interference caused and continues to cause damage to Plaintiffs.

XII. EIGHTH CAUSE OF ACTION

(Conversion)

138. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

139. Vickery intentionally and without authorization gained access to confidential and sensitive information stored on River City's private computer network, which at all relevant times operated in and affected interstate and foreign commerce and is accordingly considered a protected computer.

140. Without authorization or permission, Vickery obtained tens of

thousands of confidential, proprietary, and sensitive business records, including account credentials, client records, email lists, and other records containing sensitive business and personal information.

141. Vickery undertook these actions personally, and with the knowledge, approval and/or ratification of Kromtech, CXO, Ragan, and the remaining defendants.

142. Defendants used unlawfully acquired account credentials to log into Plaintiffs' PayPal account and convert Plaintiffs' funds stored therein.

143. As a result of such conversion, each Plaintiff suffered and continues to suffer damages.

XIII. NINTH CAUSE OF ACTION

(Intentional Infliction of Emotional Distress)

144. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

145. Defendant Vickery is not an employee or authorized user of River City's computer networks.

146. Vickery intentionally and without authorization gained access to confidential and sensitive information stored on River City's private computer network, which at all relevant times operated in and affected interstate and foreign commerce and is accordingly considered a protected computer.

147. Without authorization or permission, Vickery obtained tens of thousands of confidential, proprietary, and sensitive business records, including account credentials, client records, email lists, and other records containing sensitive business and personal information.

148. Vickery took all such actions knowingly and intentionally and without regard for the rights of others.

149. Vickery undertook these actions personally, and with the knowledge, approval and/or ratification of Kromtech, CXO, Ragan, and the remaining

defendants.

150. Defendants' illegal hacking conduct is extreme and outrageous and utterly intolerable in a civilized community.

151. Defendants intentionally inflicted emotional distress upon the non-corporate Plaintiffs.

152. Each non-corporate Plaintiff suffered and continues to suffer severe emotional distress.

153. As a result of such emotional distress, each non-corporate Plaintiff suffered and continues to suffer damages.

XIV. TENTH CAUSE OF ACTION

(Defamation)

154. Plaintiffs hereby incorporate by reference the foregoing paragraphs as though fully set forth herein.

155. Defendants published, in writing, false and defamatory statements regarding, for example, the character, nature, and legality of Plaintiffs' business operations, business model, and Plaintiffs' actions related thereto.

156. Defendants knew or should have known that such statements were false at the time they were made.

157. Defendants' communications were not privileged in any manner recognized by law.

158. Defendants' defamatory statements directly injured and continue to injure Plaintiffs' reputation in their profession, trade, and business.

159. Defendants' defamatory statements directly injured and continue to injure the perception of each non-corporate Plaintiff's moral character.

160. As a result of such defamation, each Plaintiff suffered and continues to suffer damages.

XV. JURY DEMAND

Plaintiffs demand a jury for all claims so triable.

XVI. REQUEST FOR RELIEF

Plaintiffs respectfully request the following relief:

1. Under the First Claim for Violation of the Computer Fraud and Abuse Act, against all Defendants:

   a. Temporary, preliminary and permanent injunctive relief;

   b. General damages to be proved at trial;

   c. Special damages to be proved at trial;

   d. Pre- and post-judgment interest thereon;

   e. The cost of responding to the offense, conducting a damage assessment, restoring or replacing the impaired data or system to its prior condition, lost revenues, and other costs incurred as a result thereof; and

   f. Such other and further relief as the Court deems just and proper.

2. Under the Second Claim for Violation of the Stored Communications Act, against all Defendants:

   a. Temporary, preliminary and permanent injunctive relief;

   b. General damages to be proved at trial;

   c. Special damages to be proved at trial;

   d. Pre- and post-judgment interest thereon;

   e. Exemplary or punitive damages;

   f. Attorneys' fees and associated costs of suit; and

   g. Such other and further relief as the Court deems just and proper.

3. Under the Third Claim for Violations of the Defend Trade Secrets Act, against all Defendants:

   a. Temporary, preliminary and permanent injunctive relief;

   b. General damages to be proved at trial;

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

c. Special damages to be proved at trial;

d. Pre- and post-judgment interest thereon;

e. Exemplary or punitive damages; and

f. Such other and further relief as the Court deems just and proper.

4. Under the Fourth Claim for Violations of the Electronic Communications Privacy Act, against all Defendants:

a. Temporary, preliminary and permanent injunctive relief;

b. General damages to be proved at trial;

c. Special damages to be proved at trial;

d. Pre- and post-judgment interest thereon;

e. Exemplary or punitive damages;

f. Attorneys' fees and associated costs of suit; and

g. Such other and further relief as the Court deems just and proper.

5. Under the Fifth Claim for Invasion of Privacy, against all Defendants:

a. Temporary, preliminary and permanent injunctive relief;

b. General damages to be proved at trial;

c. Special damages to be proved at trial;

d. Pre- and post-judgment interest thereon;

e. Exemplary or punitive damages; and

f. Such other and further relief as the Court deems just and proper.

6. Under the Sixth Claim for Intentional Interference with Contractual Relations, against all Defendants:

a. Temporary, preliminary and permanent injunctive relief;

b. General damages to be proved at trial;

c. Special damages to be proved at trial;

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

d. Pre- and post-judgment interest thereon;

e. Exemplary or punitive damages; and

f. Such other and further relief as the Court deems just and proper.

7. Under the Seventh Claim for Intentional Interference with a Business Expectancy, against all Defendants:

a. Temporary, preliminary and permanent injunctive relief;

b. General damages to be proved at trial;

c. Special damages to be proved at trial;

d. Pre- and post-judgment interest thereon;

e. Exemplary or punitive damages; and

f. Such other and further relief as the Court deems just and proper.

8. Under the Eighth Claim for Conversion, against All Defendants:

a. General damages to be proved at trial;

b. Special damages to be proved at trial;

c. Pre- and post-judgment interest thereon; and

d. Such other and further relief as the Court deems just and proper.

9. Under the Ninth Claim for Intentional Infliction of Emotional Distress, against all Defendants:

a. Temporary, preliminary and permanent injunctive relief;

b. General damages to be proved at trial;

c. Special damages to be proved at trial;

d. Pre- and post-judgment interest thereon;

e. Exemplary or punitive damages; and

f. Such other and further relief as the Court deems just and proper.

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

10. Under the Tenth Claim for Defamation, against all Defendants:

a. Temporary, preliminary and permanent injunctive relief;

b. General damages to be proved at trial;

c. Special damages to be proved at trial;

d. Pre- and post-judgment interest thereon;

e. Exemplary or punitive damages; and

f. Such other and further relief as the Court deems just and proper.

Respectfully submitted May 31, 2018.

NEWMAN DU WORS LLP

Jason E. Bernstein, WSBA #39362
jake@newmanlaw.com
Leeor Neta, *admitted pro hac vice*
leeor@newmanlaw.com
2101 Fourth Avenue, Suite 1500
Seattle, WA 98121
(206) 274-2800

Attorneys for Plaintiffs